I CLAIM:

1. A method for providing increased trust for secure relationship-based transactions between (1) a client using a client computer microprocessor platform and (2) at least one remote server, comprising the steps of:

(a) employing a trusted server configured to accept at least one public key datum, wherein each said public key datum is specifically associated with the client platform as part of a public/private key pair for the platform, wherein each said public/private key pair may be generated using at least one of: (i) the client platform; or (ii) the trusted server;

(b) associating additional approval data with said public key datum to identify said public key datum as having been approved by the trusted server which accepts said public key datum;

(c) making available to the remote server said public key datum and said associated additional approval data, the remote server being configured to recognize trustworthy additional approval data from said trusted server for approval of said public key datum as trustworthy;

(d) associating remote server-specific data with said approved public key datum, wherein said associated remote server-specific data is used in conjunction with the client platform private key associated with said public key datum, wherein through client platform communication with said trusted server, said trusted server is made aware of at least one utilization of the client platform private key with server-specific data from said remote server, giving said trusted server opportunity to accept or

reject the association of said public key datum with said remote server, and to provide or deny an assurance.

2. A method for enhancing trust for transactions between (1) a client using a client computer microprocessor platform and (2) a remote server, the method employing at least one trusted server, the method comprising the steps of:

(a) transferring data from the remote server to a trusted server, said transferred data including at least one secret datum, wherein said transfer is effected in conjunction with data transfer security provisions;

(b) providing from said trusted server to the client platform a function of a portion of said transferred data, wherein said portion includes at least a part of said at least one secret datum, wherein the transferring trusted server provides a value of said function to the client platform encrypted by at least one key recognizable by said trusted server as associated with the client platform deemed trustworthy, the client platform being operational to decrypt said encrypted function value; and

(c) allowing said value of said function to be securely shared between the remote server and the client platform.

3. The method of claim 2, wherein said value of said function provided to the client platform from said trusted server is dependent on attributes of the client platform as known to said trusted server

4. A method for trusted delivery of computer object data to a client computer microprocessor platform, wherein a remote server supplies source data of which the delivered object data is a function, the method comprising the steps of:

(a) identifying a secret datum, distinct from the object data, that is known to the remote server, said secret datum being made available to a trusted server and being identified with a unique tag;

(b) causing source data to be submitted to said trusted server in association with said unique tag;

(c) providing for use at a client platform the computer object data derived from said submitted source data, wherein the object data is associated with a signature computed by said trusted server, and wherein said signature is a function f_1 of said object data.

5. The method of claim 4, wherein said signature further comprises:

(ii) a function f_2 of the object data, and wherein calculation of said function f_2 of the object data given knowledge of the object data requires accurate knowledge of said secret datum.

6. The method of claim 4, wherein said signature further comprises:

(ii) a function f_2 of data, wherein a function value is available to said trusted server, and wherein a function f_3 of data is provided to the remote server, and

wherein calculation of said function f_2 of data given knowledge of function f_3 of said data and knowledge of the object data requires accurate knowledge of said secret datum.

7. The method of claim 6, wherein said data is generated at least in part randomly by said trusted server.

8. The method of claim 6, wherein computation of said function f_2 of said data given knowledge of said data and knowledge of the object data requires accurate knowledge of said secret datum.

9. The method of claim 6, wherein computation of said function f_3 of said data given knowledge of said data and knowledge of the object data requires accurate knowledge of said secret datum.

10. A method for providing control of computer object data deriving from source data associated with a remote server, the object data being usable by a plurality of clients using client computer microprocessor platforms, comprising the steps of:

(a) identifying a first datum associated with a unique tag, said first datum and associated tag being known to the remote server;

(b) associating with said first datum and tag a second datum, said second datum being provided by a trusted server which is configured to store information reflecting said first datum and tag and said second datum;

(c) binding computer object data to a value computed as a function of a derived datum, wherein said derived datum comprises at least one of (A) data indicative of said first datum and (B) data indicative of said second datum, wherein said binding is performed by said trusted server;

(d) associating for the remote server: (i) additional data of the remote server; with (ii) at least one of (C) data indicative of said first datum and (D) data indicative of said second datum; and with (iii) said associated tag, to form an additional data bundle;

(e) submitting said additional data bundle to said trusted server and if said bundle is verified as consistent with said stored information regarding said first datum and tag and said second datum as stored by the trusted server, associating said derived datum with functions of said data bundle for delivery to a client platform.

11. The method of claim 10, wherein said first datum comprises a secret datum.

12. The method of claim 10, wherein said derived datum comprises an encryption key.

13. The method of claim 10, wherein said first datum comprises a secret datum and said derived datum comprises an encryption key.

14. A method for providing control of computer object data deriving from source data associated with a remote server, the object data being usable by a plurality of clients using client computer microprocessor platforms, comprising the steps of:

(a) identifying a first datum associated with a unique tag, said first datum and associated tag being known to the remote server;

(b) binding computer object data to a value computed as a function of a derived datum, wherein said derived datum comprises data indicative of said first datum, wherein said binding is performed by a trusted server wherein said trusted server is configured to store information reflecting said first datum and tag;

(c) associating for the remote server: (i) additional data of the remote server, including data indicative of said first datum; with (ii) said associated tag, to form an additional data bundle;

(d) submitting said additional data bundle to said trusted server and if said bundle is verified as consistent with said stored information regarding said first datum and tag as stored by the trusted server, associating said derived datum with functions of said data bundle for delivery to a client platform.

15. The method of claim 14, wherein said first datum comprises a secret datum.

16. The method of claim 14, wherein said derived datum comprises an encryption key.

17. The method of claim 14, wherein said first datum comprises a secret datum and said derived datum comprises an encryption key.

18. A system for providing increased trust for secure relationship-based transactions, comprising:

a at least one remote server;

b a data communications link operationally coupled with said at least one remote server;

c a trust server configured to accept at least one public key datum operationally coupled with said data communications link;

d a client computer microprocessor platform operationally coupled with said trust server, wherein said client computer microprocessor platform is supplied with programming operable to

i employ said trusted server configured to accept at least one public key datum, wherein each said public key datum is specifically associated with the client platform as part of a public/private key pair for the platform, wherein each said public/private key pair may be generated using at least one of: (i) the client platform; or (ii) the trusted server;

ii associate additional approval data with said public key datum to identify said public key datum as having been approved by the trusted server which accepts said public key datum;

iii make available to the remote server said public key datum and said associated additional approval data, the remote server being configured to recognize trustworthy additional approval data from said trusted server for approval of said public key datum as trustworthy;

iv associate remote server-specific data with said approved public key datum, wherein said associated remote server-specific data is used in conjunction with the client platform private key associated with said public key datum, wherein through client platform communication with said trusted server, said trusted server is made aware of at least one utilization of the client platform private key with server-specific data from said remote server, giving said trusted server opportunity to accept or reject the association of said public key datum with said remote server, and to provide or deny an assurance.

19. A system for providing increased trust for secure relationship-based transactions, comprising:

a at least one remote server;

b a data communications link operationally coupled with said at least one remote server;

c a client computer microprocessor platform operationally coupled with said data communications link,

d a trusted server operationally coupled with said data communications link, wherein said trust server is supplied with programming operable to

i transfer data from the remote server to the trusted server, said transferred data including at least one secret datum, wherein said transfer is effected in conjunction with data transfer security provisions;

ii provide from said trusted server to the client computer microprocessor platform a function of a portion of said transferred data, wherein said portion includes at least a part of said at least one secret datum, wherein the transferring trusted server provides a value of said function to the client platform encrypted by at least one key recognizable by said trusted server as associated with the client platform deemed trustworthy, the client platform being operational to decrypt said encrypted function value; and

iii allow said value of said function to be securely shared between the remote server and the client platform.

20. The system of claim 19, wherein said value of said function provided to the client computer microprocessor platform from said trusted server is dependent on attributes of the client computer microprocessor as known to said trusted server.

21. A system for trusted delivery of computer object data, comprising:

a at least one remote server;

b a data communications link operationally coupled with said at least one remote server;

c a client computer microprocessor platform operationally coupled with said data communications link,

d a trusted server operationally coupled with said data communications link, wherein said trust server and said client computer microprocessor platform are supplied with programming together operable to

i identify a secret datum, distinct from the object data, that is known to the remote server, said secret datum being made available to a trusted server and being identified with a unique tag;

ii cause source data to be submitted to said trusted server in association with said unique tag;

iii provide for use at a client computer microprocessor platform the computer object data derived from said submitted source data,

wherein the object data is associated with a signature computed by said trusted server, and wherein said signature is a function f_1 of said object data.

22. The system of claim 21, wherein said signature further comprises a function f_2 of the object data, and wherein calculation of said function f_2 of the object data given knowledge of the object data requires accurate knowledge of said secret datum.

23. The system of claim 21, wherein said signature further comprises a function f_2 of data, wherein a function value is available to said trusted server, and wherein a function f_3 of data is provided to the remote server, and wherein calculation of said function f_2 of data given knowledge of function f_3 of said data and knowledge of the object data requires accurate knowledge of said secret datum.

24. The system of claim 23, wherein said data is generated at least in part randomly by said trusted server.

25. The system of claim 23, wherein computation of said function f_2 of said data given knowledge of said data and knowledge of the object data requires accurate knowledge of said secret datum.

26. The system of claim 23, wherein computation of said function f_3 of said data given knowledge of said data and knowledge of the object data requires accurate knowledge of said secret datum.

27. A system for providing control of computer object data deriving from source data associated with a remote server, comprising:

a a plurality of client computer microprocessor platforms;

b a data communications link operationally coupled with said client computer microprocessor platform;

c a trusted server operationally coupled with said data communications link, wherein said trusted server and said client computer microprocessor platform are supplied with programming operable to

i identify a first datum associated with a unique tag, said first datum and associated tag being known to the remote server;

ii associate with said first datum and tag a second datum, said second datum being provided by said trusted server which is configured to store information reflecting said first datum and tag and said second datum;

iii bind computer object data to a value computed as a function of a derived datum, wherein said derived datum comprises at least one of (A) data indicative of said first datum and (B) data indicative of said second datum, wherein said binding is performed by said trusted server;

iv associate for the remote server: (i) additional data of the remote server; with (ii) at least one of (C) data indicative of said first datum and (D) data indicative of said second datum; and with (iii) said associated tag, to form an additional data bundle;

v submit said additional data bundle to said trusted server and if said bundle is verified as consistent with said stored information regarding said first datum and tag and said second datum as stored by the trusted server, associating said derived datum with functions of said data bundle for delivery to said client computer microprocessor platform.

28. The system of claim 27, wherein said first datum comprises a secret datum.

29. The system of claim 27, wherein said derived datum comprises an encryption key.

30. The system of claim 27, wherein said first datum comprises a secret datum and said derived datum comprises an encryption key.

31. A system for providing control of computer object data deriving from source data associated with a remote server, comprising:

a a plurality of client computer microprocessor platforms;

b a data communications link operationally coupled with said client computer microprocessor platform;

c a trusted server operationally coupled with said data communications link, wherein said trusted server and said client computer microprocessor platform are supplied with programming operable to

i identify a first datum associated with a unique tag, said first datum and associated tag being known to the remote server;

ii bind computer object data to a value computed as a function of a derived datum, wherein said derived datum comprises data indicative of said first datum, wherein said binding is performed by said trusted server, and wherein said trusted server is configured to store information reflecting said first datum and tag;

iii associate for the remote server: (i) additional data of the remote server including data indicative of said first datum with (ii) said associated tag, to form an additional data bundle;

iv submit said additional data bundle to said trusted server and if said bundle is verified as consistent with said stored information regarding said first datum and tag as stored by the trusted server, associating said derived datum with functions of said data bundle for delivery to said client computer microprocessor platform.

32. The system of claim 31, wherein said first datum comprises a secret datum.

33. The system of claim 31, wherein said derived datum comprises an encryption key.

34. The system of claim 31, wherein said first datum comprises a secret datum and said derived datum comprises an encryption key.